AMENDMENTS TO THE SPECIFICATION

Please amend the specification as indicated hereafter. It is believed that the following amendments and additions add no new matter to the present application.

In the Specification: [Use ~~strikethrough~~ for deleted matter (or double square brackets "[[]]" if the strikethrough is not easily perceivable, *i.e.*, "4" or a punctuation mark) and underlined for added matter.]

Please amend the paragraph starting on p. 1, line 24 as follows:

A very popular industry standard protocol for data communication along the networks is the Internet Protocol (IP). In time, the Transmission Control Protocol (TCP) and the Unreliable Datagram Protocol (UDP) were developed for use with the IP. The former protocol (TCP/IP) is a protocol which guarantees transfer of data without errors, as it implements certain check functionality, and the latter protocol (UDP/IP) is a protocol which does not guarantee transfer of data, but requires ~~must~~ much less overhead than the TCP/IP platform. Furthermore, in order to keep track of and manage the various devices situated on a network, the simple network management protocol (SNMP) was eventually developed for use with the UDP/IP platform. The use of the foregoing protocols has become extensive in the industry, and numerous venders manufacture many types of networks devices which can employ these protocols.

Please amend the paragraph starting on p. 7, line 7 as follows:

The discovery/layout software 101 implements object-oriented functionality. In the context of SNMP managers, object-oriented means that most of the management system actions and processes that the user can invoke are oriented toward a class of devices rather than individually managed network nodes. Generally, the discovery/layout software 101 of FIG. 1 is configured to discover the network topology, that is, all network node interconnections existing on the network 118, and to construct a map, comprising various sub-maps, any of which can be used for displaying the network topology on the ~~device~~ display 108.

Please amend the paragraph starting on p. 7, line 15 as follows:

FIG. 2 shows a map 200 which is generated by the discovery/layout software 101 from topology data discovered from the network 118 (FIG. 1). The discovery/layout software 101 can drive any of the various sub-maps to the display 108 (FIG. 1) for viewing by the user. The sub-maps in the map 200 of FIG. 2 are arranged in a hierarchy. A root sub-map 202 is defined at a root level. The root sub-map 202 represents the highest logical level sub-map in the hierarchy and shows objects 203 as anchor points for different sub-map hierarchies. Each hierarchy is a separate management domain. This could be, for instance, a network, logical grouping of nodes, or some other domain. An Internet sub-map 204 is defined at an Internet level and is generated by exploding an object 203 within the root sub-map 202. "Exploding" in the context in this document means that the user prompts the management station 100 with the input device 106 (FIG. 1) to breakdown and provide more data pertaining to the object 203 at issue. Further, the Internet sub-map 204 illustrates objects 203 in the form of networks and routers. Any one of a number of network sub-maps 206 can be exploded from the Internet sub-map 204. Each network sub-map 206 shows objects 203 in the form of segments and connectors. Any one of a number of segment sub-maps 208 can be exploded from an object 203 within a network sub-map. Each segment sub-map 208 shows objects in the form of network nodes. Finally, any one of a number of node sub-maps 210 can be exploded from an object 203 within a segment sub-map 208. Each node sub-map 210 shows objects 203 in the form of interfaces within that node.

Please amend the paragraph starting on p. 9, line 3 as follows:

The network monitor 306 transmits and receives data packets to and from the network 118. The network monitor 386 discovers and monitors network topology, as indicated by arrows 308a, 308b. When network topology changes on the network, the network monitor 306 generates events, or "traps" (SNMP vernacular), which include an object identifier and object change information. The network monitor 306 can also receive events from other devices, such as a router, in the network 118. The network monitor 306 interacts with the network 118 by way of the network software 124 (FIG. 1), which essentially comprises protocol stacks, corresponding to IP, TCP, UDP, SNMP in the preferred embodiment, and which generally implements these protocols and performs validation functions. Furthermore, the network monitor 306 populates the topology database 314 by way of the topology manager 310 and notifies the topology manager [[31]] 310 of events (topology changes).

Finally, it should be noted that U.S. Patent No. 5,185,860, issued to *J.C. Wu*, which is incorporated herein by reference, describes a node discovery system which could be employed to implement the network monitor 306 herein.